United States District Court

NORTHERN DISTRICT OF GEORGIA

UNITED STATES OF AMERICA
v.
CHRISTOPHER DOBBINS

CRIMINAL COMPLAINT

Case Number: 1:20-MJ-315

I, the undersigned complainant being duly sworn, state the following is true and correct to the best of my knowledge and belief. On or about March 29, 2020, in the Northern District of Georgia, the defendant, CHRISTOPHER DOBBINS, knowingly caused and attempted to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused and attempted to intentionally cause damage without authorization to a protected computer–that is, one or more computers used by [COMPANY-1][1] to conduct its business–and the offense caused and would, if completed, have caused: (i) loss, aggregating at least $5,000 in value, to [COMPANY-1] during the one year period beginning on or about March 29, 2020, from DOBBINS's course of conduct affecting a protected computer; (ii) the modification, impairment, and potential modification and impairment of the medical examination, diagnosis, treatment and care of one or more individuals; and (iii) a threat to public health and safety; in violation of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and (c)(4)(B).

I further state that I am a(n) Special Agent of the Federal Bureau of Investigation and that this complaint is based on the following facts:

PLEASE SEE ATTACHED AFFIDAVIT

Continued on the attached sheet and made a part hereof. Yes

Signature of Complainant
Roderick F. Coffin

Based upon this complaint, this Court finds that there is probable cause to believe that an offense has been committed and that the defendant has committed it. Sworn to me by telephone pursuant to Federal Rule of Criminal Procedure 4.1.

April 15, 2020
Date

at Atlanta, Georgia
City and State

RUSSELL G. VINEYARD
UNITED STATES MAGISTRATE JUDGE
Name and Title of Judicial Officer

Russell G. Vineyard
Signature of Judicial Officer

AUSA S. Kaushal / 2020R00352

[1] In this complaint and attached affidavit, the victim company's name has been replaced with a generic identifier to protect its identity.

AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT

I, Roderick F. Coffin, depose and say under penalty of perjury:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of a criminal complaint and arrest warrant for Christopher Dobbins. As discussed below, I believe that there is probable cause to believe that Dobbins committed violations of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and (c)(4)(B).

2. I am a Special Agent with the FBI and have been since June 2010. I am currently assigned to the Atlanta Field Office Cyber Crimes squad. My current duties include the full-time investigation of computer crimes, and I have participated in numerous investigations involving computer and technology related crimes including computer intrusions and internet fraud. I have also received specialized training in the federal criminal statutes that relate to computer intrusions and other computer-related crimes, and in the investigation of these offenses. Prior to my employment with the FBI, I worked for approximately 12 years in the computer industry, specializing in software development and software development consulting.

3. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information I obtained from others, including witnesses. Because this affidavit is being submitted for the limited purpose of establishing probable cause, I have not included in this affidavit every detail of every aspect of the investigation. Rather, I have set forth facts that I believe are sufficient to establish probable cause for the issuance of the requested criminal complaint and arrest warrant. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

RELEVANT STATUTE

4. Title 18, United States Code, Section 1030, entitled "Fraud and related activity in connection with computers," states, in relevant part:

> (a) Whoever—
> . . .
> (5)
> (A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
> . . .
> shall be punished as provided in subsection (c) of this section.

18 U.S.C. § 1030(a)(5)(A). Attempts to commit this crime are also violations of federal law. 18 U.S.C. § 1030(b).

5. A violation of Section 1030(a)(5)(A) is a felony if the offense conduct caused (or in the case of an attempted offense, would, if completed, have caused):

> (I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
>
> (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; [or] . . .
>
> (IV) a threat to public health or safety[.]

18 U.S.C. §§ 1030(c)(4)(A)(i) and (c)(4)(B).

TECHNICAL TERMS

6. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. IP Address: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

b. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

PROBABLE CAUSE

A. Starting on March 29, 2020, a computer intrusion at [COMPANY-1][1] began delaying the shipment of Personal Protective Equipment ("PPE").

7. On or about April 7, 2020, [COMPANY-1] reported to the FBI that it had experienced an intrusion into its computer network and that the intruder deleted records causing disruption to its operations. [COMPANY-1] specializes in packaging and

[1] The victim company's name has been replaced with a generic identifier to protect its identity.

distributing medical devices and procedure trays to healthcare providers, including Personal Protective Equipment ("PPE") such as gloves, masks, and gowns. [COMPANY-1] has offices in Peachtree Corners, Georgia, and Waukegan, Illinois.

8. I know that, as of March 29, 2020, the United States was in the middle of a global pandemic caused by Coronavirus (COVID-19) and PPEs were, and remain today, in extremely high demand for first responders, medical professionals, and citizens throughout the country.

9. According to [COMPANY-1], the intrusion was detected on or around March 29, 2020, when [COMPANY-1] experienced technical difficulties while attempting to print shipping labels for product shipments to customers. These technical difficulties, according to [COMPANY-1], delayed shipments of PPEs to customers during the midst of a global pandemic.

10. [COMPANY-1] utilizes Oracle's NetSuite Enterprise Resource Planning ("ERP") and Customer Relationship Management ("CRM") applications to manage many aspects of its business operations, including sales, invoicing, inventory, and shipment. Based on my training and experience, I know that ERP and CRM applications provide a wide range of functionality that are typically important to business operations.

11. [COMPANY-1] investigated the shipping labels issue and determined that the NetSuite forms that [COMPANY-1] uses to print shipping labels had been deleted by an intruder. [COMPANY-1]'s investigation further revealed that the intruder modified approximately 115,581 NetSuite records and deleted approximately 2,371 records. [COMPANY-1]'s investigation also indicated that the intruder was former [COMPANY-1] Vice President of Finance Christopher Dobbins.

B. The evidence shows that Christopher Dobbins, a recently fired employee, was responsible for the computer intrusion.

12. According to [COMPANY-1], Dobbins was hired by [COMPANY-1] as their Vice President of Finance on August 1, 2016, and was integral in setting up

[COMPANY-1]'s NetSuite applications. Dobbins was [COMPANY-1]'s main NetSuite contact and had responsibilities for adding and removing users from NetSuite. Due to conflicts between Dobbins and other departments within [COMPANY-1], Dobbins was disciplined by [COMPANY-1] on August 9, 2019, and December 16, 2019; and fired by [COMPANY-1] on March 2, 2020.

13. [COMPANY-1]'s investigation has revealed a pattern of escalating abuse of its NetSuite applications by Dobbins that appears to coincide with [COMPANY-1]'s disciplinary actions against Dobbins.

14. Specifically, Dobbins was disciplined on or about August 9, 2019. According to NetSuite audit logs provided by [COMPANY-1] to the FBI, on August 13, 2019 at 8:03 AM, Dobbins's NetSuite account was logged in from [COMPANY-1]'s network and created a fictitious user account in the name of "Jagdish Kavitha" and having the email address jagdishkavitha82@gmail.com. According to [COMPANY-1], no person named Jagdish Kavitha has ever been employed by [COMPANY-1] and, to access administrative functions of NetSuite, an administrator must possess both valid credentials (username and password) and a second form of authentication.

15. I believe that it is highly likely that Dobbins created the Kavitha NetSuite account because:

a. The creation of the account came from [COMPANY-1]'s network;

b. The creator possessed Dobbins's username, password, and second form of authentication; and

c. Dobbins had responsibility at [COMPANY-1] to manage NetSuite user accounts.

16. On December 16, 2019, Dobbins was again disciplined by [COMPANY-1] and Dobbins's NetSuite access was disabled at 9:18 AM. At 10:03 AM, the Kavitha NetSuite account was logged in from IP address 47.36.49.135. According to NetSuite audit records reviewed by the FBI, IP address 47.36.49.135 also accessed Dobbins's

NetSuite account approximately 952 times between May 24, 2018, and February 29, 2020. I therefore believe that IP address 47.36.49.135 was commonly used by Dobbins and that the December 16, 2019, Kavitha login was performed by Dobbins.

17. According to publicly available information, IP address 47.36.49.135 is registered to Charter Communications ("Charter") and services the North Atlanta area. In response to a subpoena, Charter provided the following subscriber information for IP address 47.36.49.135:

Name:	Dobbins Consulting
Address:	[redacted] [redacted]
Lease Start:	9/14/2019
Lease End:	4/7/2020

18. I have conducted a search of Georgia drivers' records and have located a driver's license for Dobbins that lists [redacted] as his residence.

19. I believe that it is highly likely that Dobbins accessed the Kavitha NetSuite account on December 16, 2019, because:

a. It is highly likely that Dobbins created the Kavitha NetSuite account;

b. Dobbins consistently accessed his legitimate NetSuite account from IP address 47.36.49.135;

c. Information provided by Charter identifies the subscriber for IP address 47.36.49.135 as "Dobbins Consulting" and the service address as the address listed on Dobbins's driver's license (minus the "SB" that appears in the Charter records); and

d. The Kavitha NetSuite account was accessed on December 16, 2019, from IP address 47.36.49.135.

20. On March 2, 2020, Dobbins was fired by [COMPANY-1] and at 4:51 PM that day his NetSuite access was terminated.

21. On March 4, 2020, at 8:20 AM the Kavitha NetSuite account was logged in from IP address 169.57.165.67. According to publicly available records, IP address 169.57.165.67 is associated with TorGuard Virtual Private Network ("VPN"). Based on my training and experience, I know that VPNs such as TorGuard can be used by computer criminals to obscure the true IP address of their Internet access.

22. On March 26, 2020, Dobbins received his last severance check from [COMPANY-1].

23. On March 29, 2020, the Kavitha NetSuite account was logged in from IP address 45.133.180.130. According to publicly available records, IP address 45.133.180.130 is also associated with TorGuard. The Kavitha NetSuite account created a fictitious user account in the name of "dbh marq" and having the email address dbhmarqf@pokemail.net. Based on my training, experience, and research, I know that pokemail.net is an email service provider that offers disposable email accounts. The website for pokemail.net states that it provides "Disposable, location-based E-Mail Address. No signup needed. Emails last 1 hour." Pokemail.net, About, https://grr.la/mail/pokemail.net (last visited Apr. 7, 2020). A few minutes after the dbh marq account is created, that account is used to log into the [COMPANY-1] Netsuite applications using IP address 45.133.180.130—the same IP address used by the Kavitha Netsuite account. And in the following 45 minutes, the dbh marq account is used to cause 115,581 record edits and 2,371 deletions. After those actions are completed, the dbh marq account deactivates the Kavitha and dbh marq accounts.

24. I believe that it is highly likely that Dobbins created the dbh marq NetSuite account and modified and deleted data from [COMPANY-1]'s NetSuite applications on March 29, 2020, because:

a. It is highly likely that Dobbins created the Kavitha NetSuite account;

b. It is highly likely that Dobbins accessed the Kavitha NetSuite account from his residence at [redacted];

c. The Kavitha NetSuite account created the dbh marq NetSuite account;

d. The creation and access of the Kavitha NetSuite account follows a pattern related to Dobbins's disciplinary history at [COMPANY-1]; and

e. Dobbins had been recently fired from [COMPANY-1] and had just received his last severance check.

25. On April 7, 2020, I located a website for Christopher Ian Dobbins at www.cidobbins.com. This website lists Dobbins's employment at [COMPANY-1] as 2016-2020. I therefore believe the web site was updated on or after March 2, 2020, the date that Dobbins was fired from [COMPANY-1]. This website lists Dobbins's address as [redacted]. In discussing Dobbins's skills, the website states: "I . . . offer a comprehensive understanding of process optimization, ERP suites (including NetSuite, Oracle eBusiness, and SAP ERP[.]"

C. The computer intrusion and disruptions to [COMPANY-1]'s business occurred in the middle of a global pandemic when PPEs were crucially important to first responders, healthcare providers, and citizens.

26. As mentioned above, the deletions and edits to [COMPANY-1]'s Netsuite applications on March 29, 2020, that delayed shipment of PPEs occurred in the midst of the COVID-19 outbreak in Georgia and in the United States. By that date:

a. The World Health Organization had declared that COVID-19 was a global pandemic;

b. The President of the United States, the Governor of Georgia, and the Mayor of Atlanta had all declared public health emergencies in response to the spread of COVID-19; and

c. The Centers for Disease Control and Prevention and other public health authorities had recommended that the public engage in social distancing and avoid gatherings of more than a few people to limit community spread of COVID-19.

27. According to data from the Georgia Department of Health, as of April 14, 2020, Georgia had the following number of confirmed COVID-19 cases, hospitalizations, and deaths:

COVID-19 Confirmed Cases:	No. Cases (%)
Total	14223 (100%)
Hospitalized	2769 (19.47%)
Deaths	501 (3.52%)

https://dph.georgia.gov/covid-19-daily-status-report (last visited April 14, 2020).

28. According to data from the Georgia Department of Health, in the days leading up to March 29, 2020, the total number of COVID-19 cases in Georgia were growing by the hundreds per day:

Date	Cumulative COVID-19 Cases
3/19/2020	2,873
3/20/2020	3,272
3/21/2020	3,525
3/22/2020	3,808
3/23/2020	4,314
3/24/2020	4,801
3/25/2020	5,344
3/26/2020	5,882
3/27/2020	6,446
3/28/2020	6,861
3/29/2020	7,266

https://dph.georgia.gov/covid-19-daily-status-report (last visited April 15, 2020).

29. According to data from the Georgia Department of Health, between March 19 and 28, 2020, 121 people died in Georgia and 24 more people died on March 29:

Date	Daily COVID-19 Deaths
3/19/2020	5
3/20/2020	5
3/21/2020	20
3/22/2020	9
3/23/2020	10
3/24/2020	14
3/25/2020	17
3/26/2020	11
3/27/2020	11
3/28/2020	20
3/29/2020	24

https://dph.georgia.gov/covid-19-daily-status-report (last visited April 15, 2020).

D. The computer intrusion caused monetary loss to [COMPANY-1]; potential modification or impairment of medical examination, diagnoses, and treatment; and contributed to a threat to public health and safety.

30. According to [COMPANY-1], the monetary losses caused from the computer intrusion exceeded $5,000 in value. The losses, which are still being determined, stem from the costs of (i) responding to the computer intrusion; (ii) restoring data to its condition prior to the computer intrusion; and (iii) lost revenue and other consequential damages incurred because of interruption of business.

31. Aside from monetary damages, the computer intrusions caused (i) a potential modification or impairment of the medical examination, diagnosis, treatment, or care of at least one person and (ii) a threat to public health and safety by delaying

shipments of PPEs. Numerous news sources have reported that there is a PPE shortage in the United States. For example, on March 18, 2020, the Wall Street Journal reported that: "Hospitals across the U.S. are running out of the masks, gowns and other equipment they need to protect staff against the novel coronavirus as they struggle to take care of patients, say hospital officials, doctors and others in the industry." Melanie Evans and Khadeeja Safdar, *Hospitals facing Coronavirus Are Running Out of Masks, Other Key Equipment*, Wall Street Journal, Mar. 18, 2020, *available at* https://www.wsj.com/articles/hospitals-facing-coronavirus-are-running-out-of-masks-other-key-equipment-11584525604 (last visited Apr. 14, 2020).

32. [COMPANY-1] has also confirmed that there is a shortage of PPEs in the United States, that its customers use PPEs to treat patients, and that the PPE shortage poses a threat to public health and safety. According to [COMPANY-1], its customers include healthcare providers that rely on PPEs to protect medical professionals who are providing care to patients and recent PPE orders were driven by the COVID-19 pandemic.

33. According to [COMPANY-1], the computer intrusion caused delays of PPE shipments of approximately 24 to 72 hours. Normally, [COMPANY-1] would be able to execute same-day delivery.

CONCLUSION

34. I submit that this affidavit supports probable cause for a complaint and arrest warrant for Christopher Dobbins for violations of Title 18, United States Code, Sections 1030(a)(5)(A), (b), and (c)(4)(B).